Beep: Use Case Diagrams
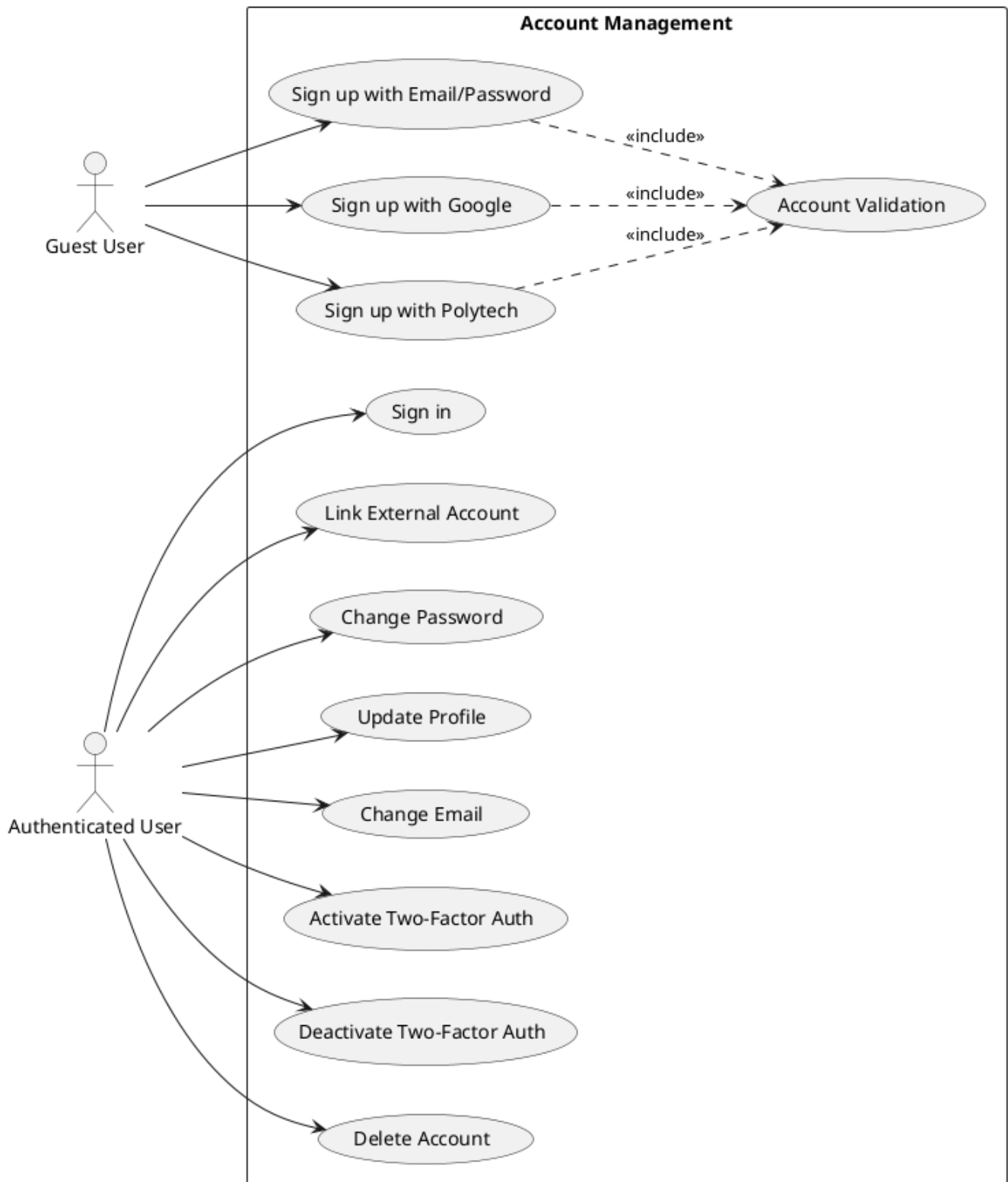
Table of Contents

End-user capabilities

This diagram shows the high-level capabilities of different user types in the system.
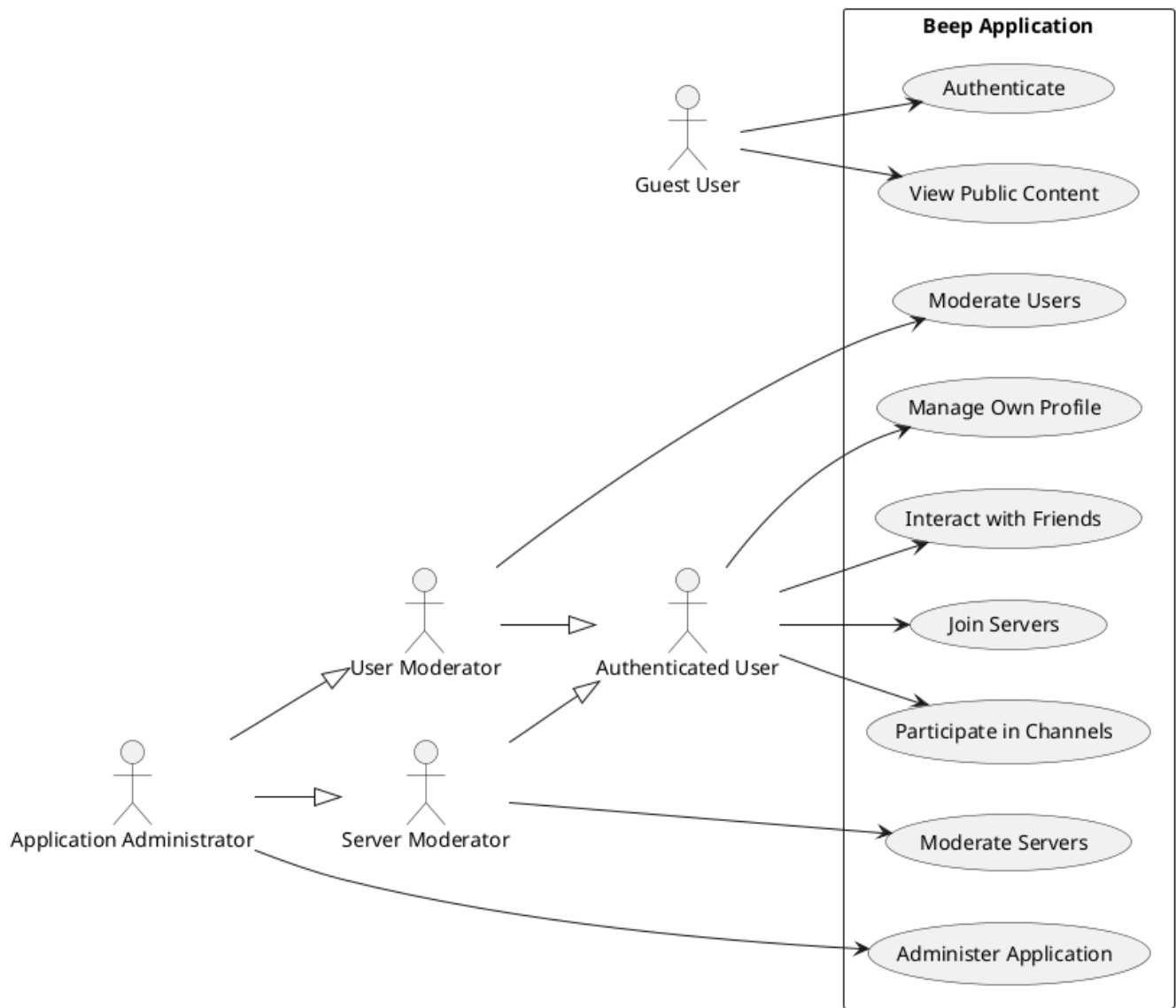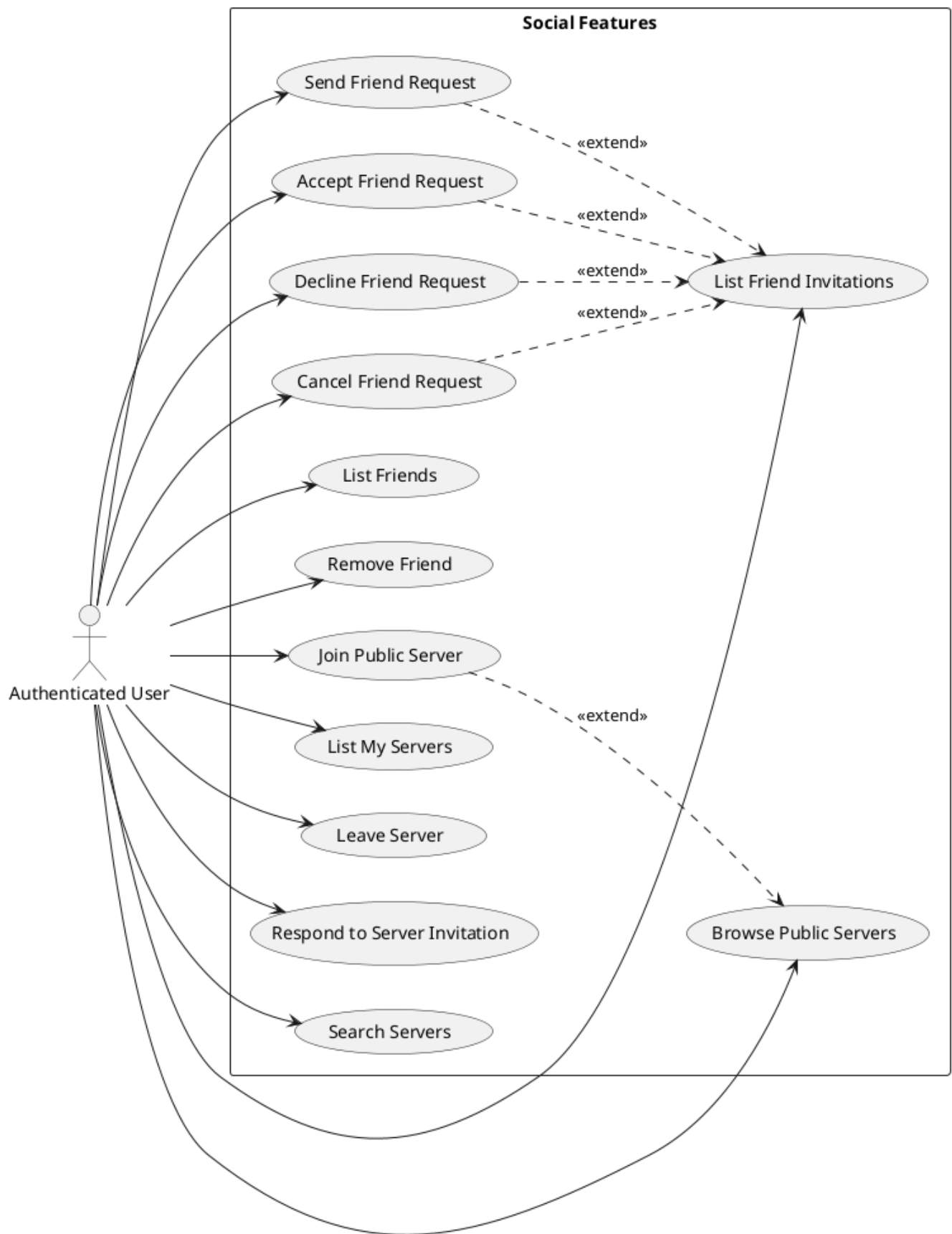
Account Management

The account management use cases detail how users manage their accounts in the system.

Social Interaction

This diagram illustrates how users interact socially within the platform.

Social Features

- Send Friend Request
- Accept Friend Request
- Decline Friend Request
- Cancel Friend Request
- List Friend Invitations
- List Friends
- Remove Friend
- Join Public Server
- List My Servers
- Leave Server
- Respond to Server Invitation
- Search Servers
- Browse Public Servers
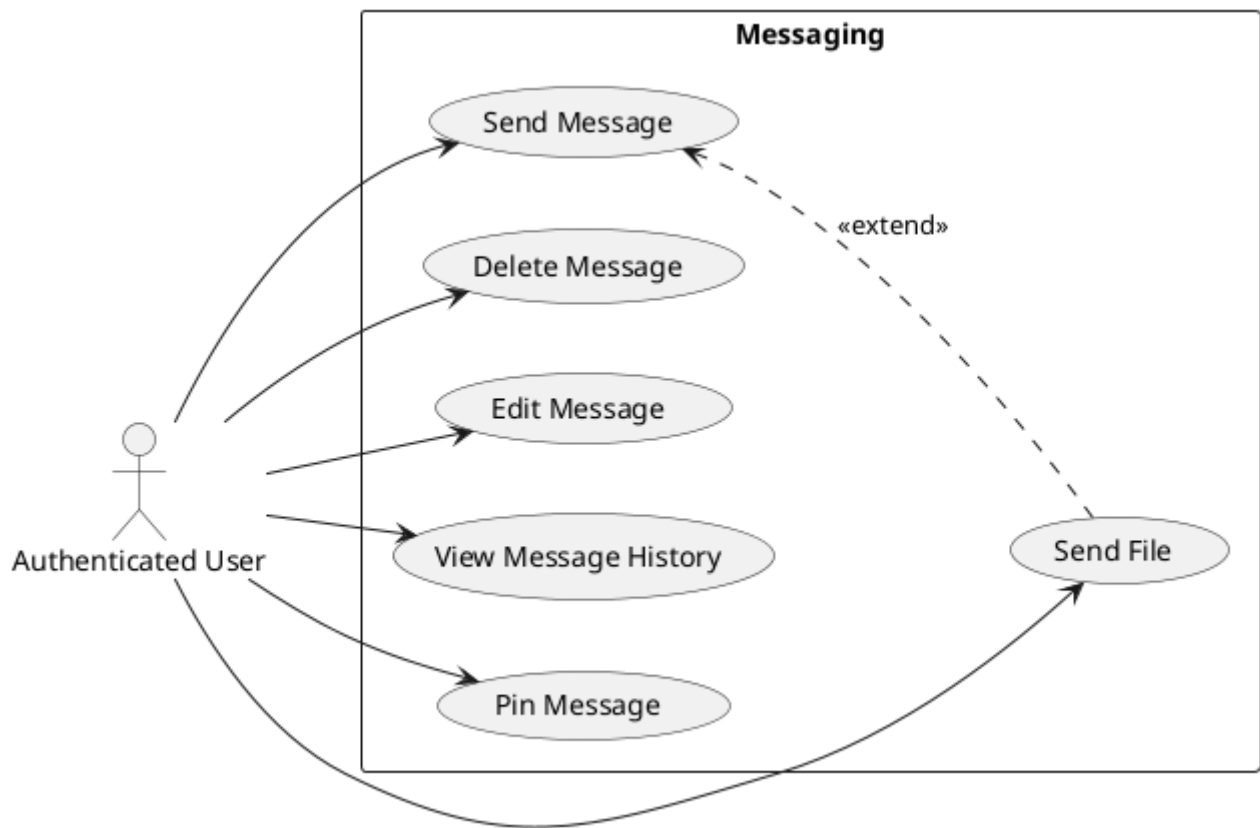
Authenticated User

«extend»

Chatting

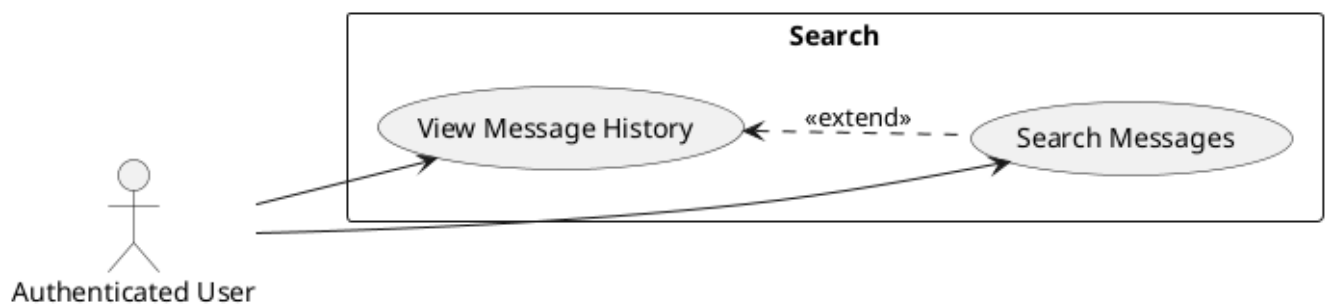This diagram shows the use cases related to chat functionality.

Channel Management
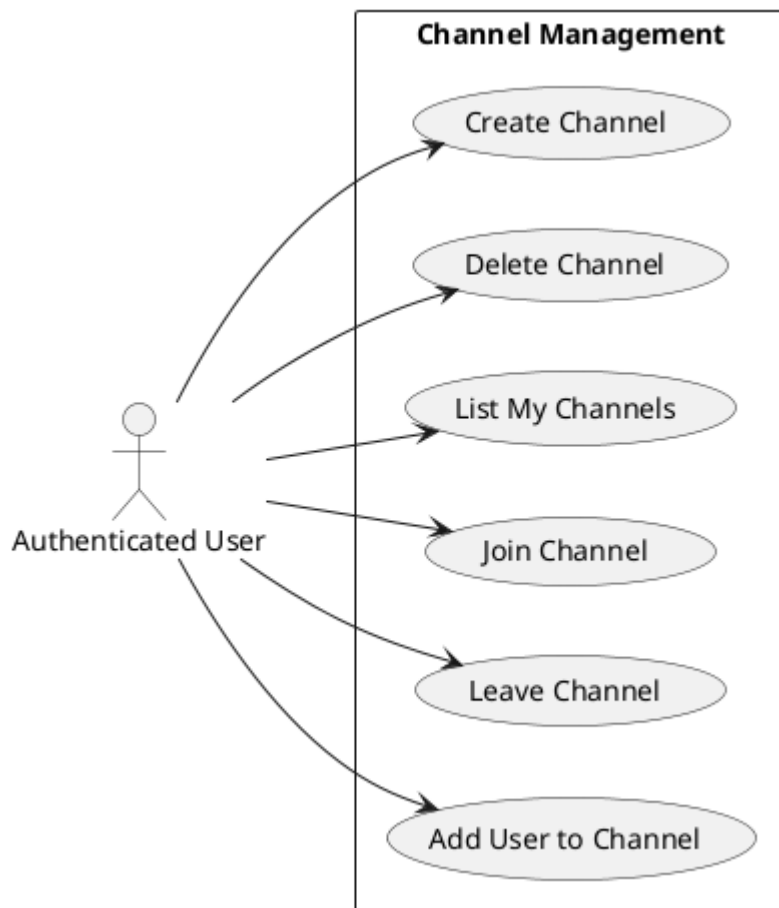
Messaging

Search

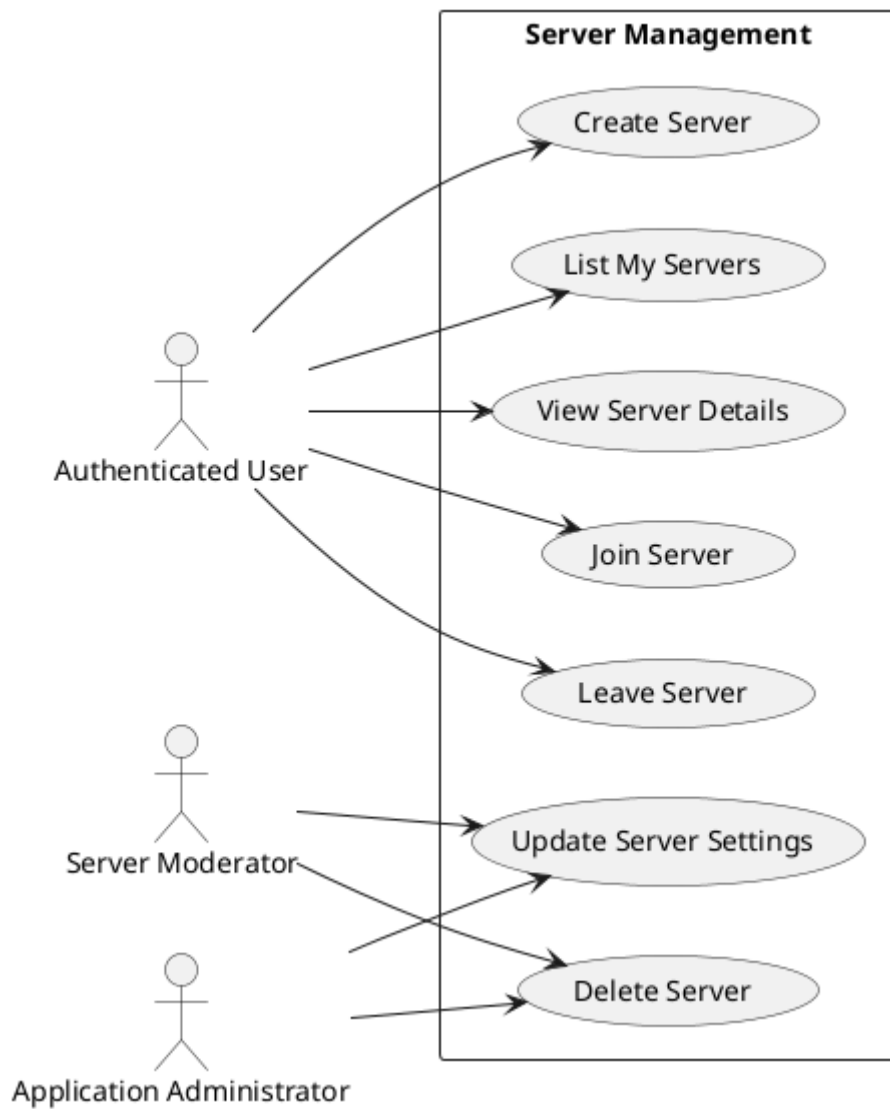# Server Management

This section describes the use cases related to server management within the application.

System Architecture Components

This diagram illustrates the microservice components of the Beep platform and their interactions.
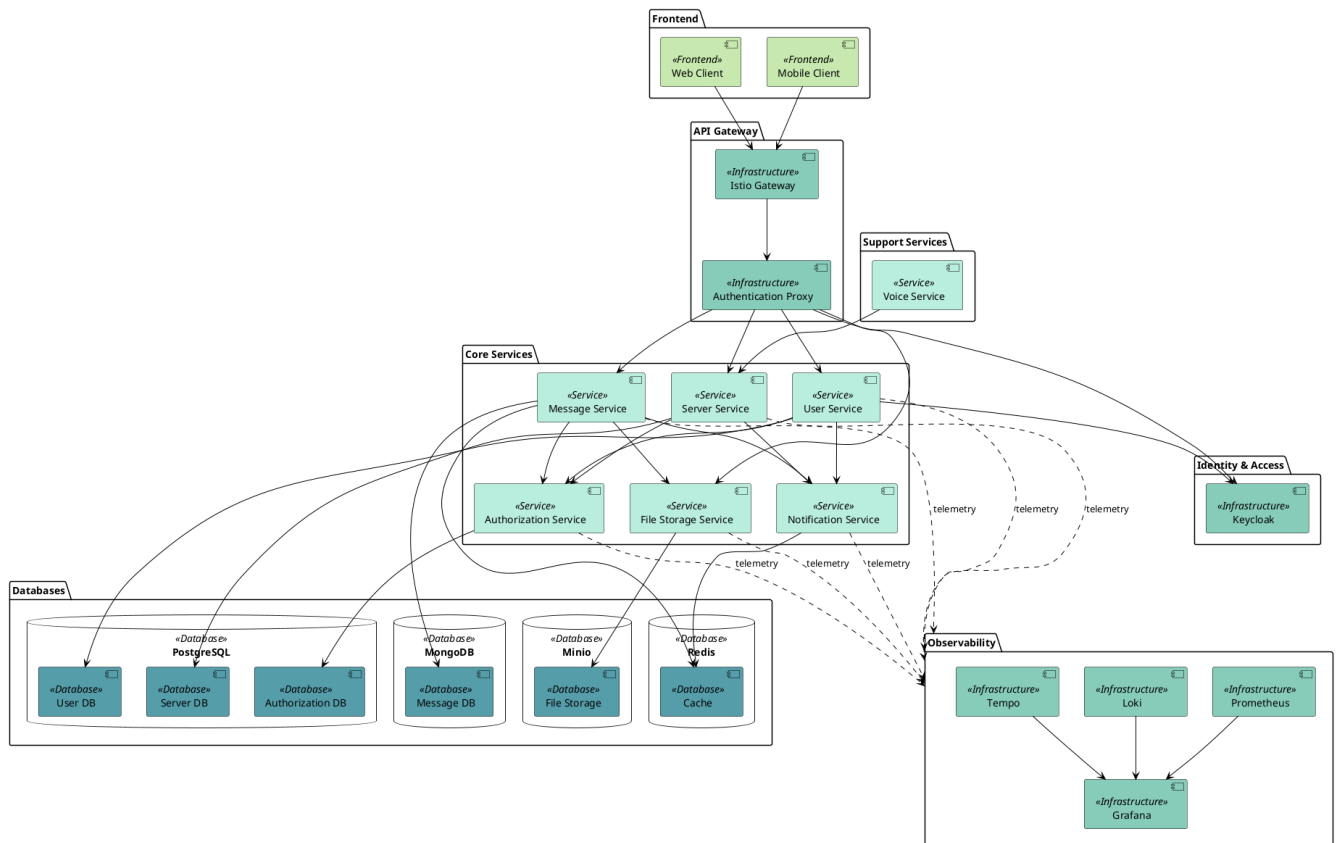
Data Flow Diagrams

This section contains diagrams illustrating key data flows within the system.

Friend Request Workflow
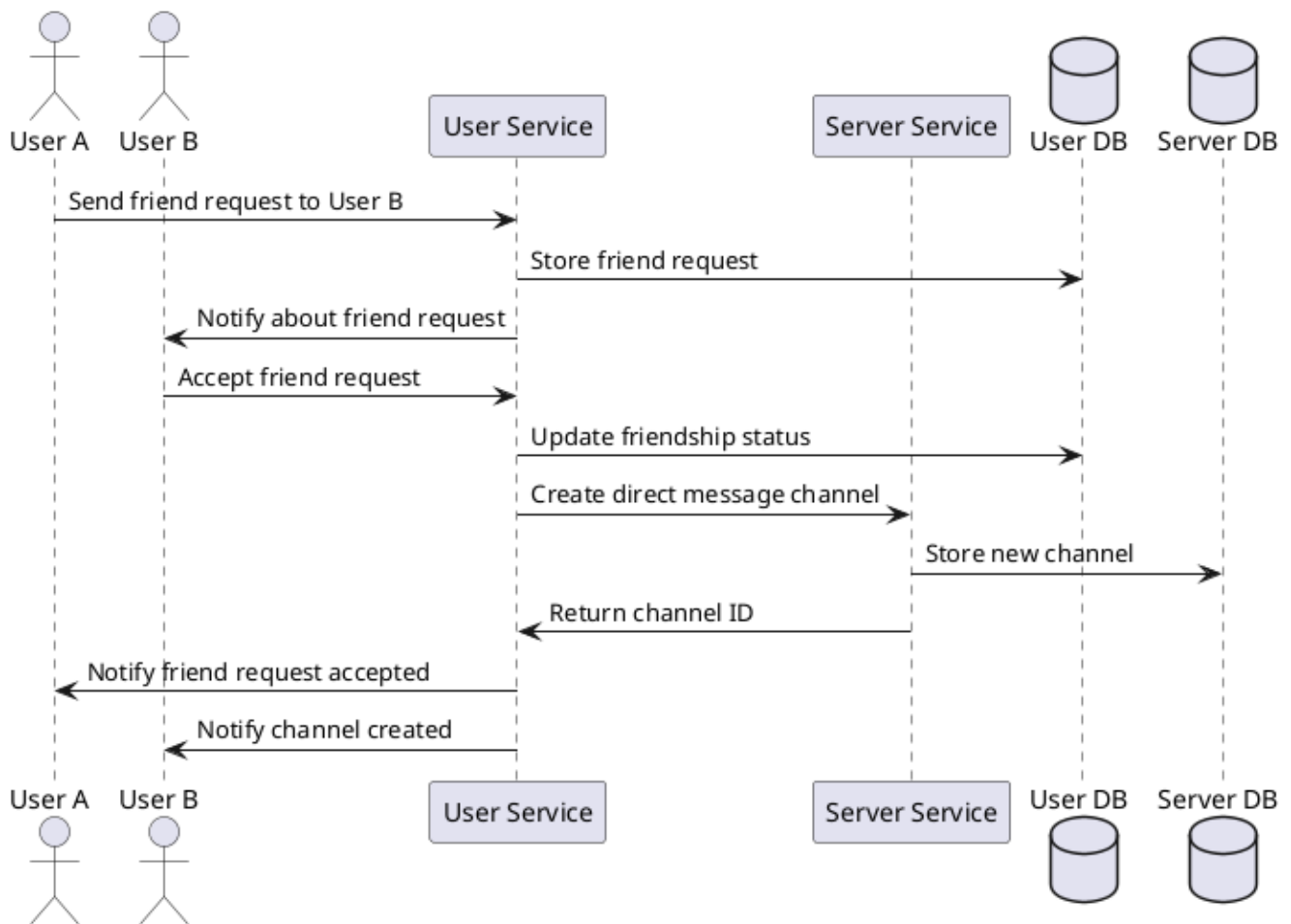
Server Creation Workflow
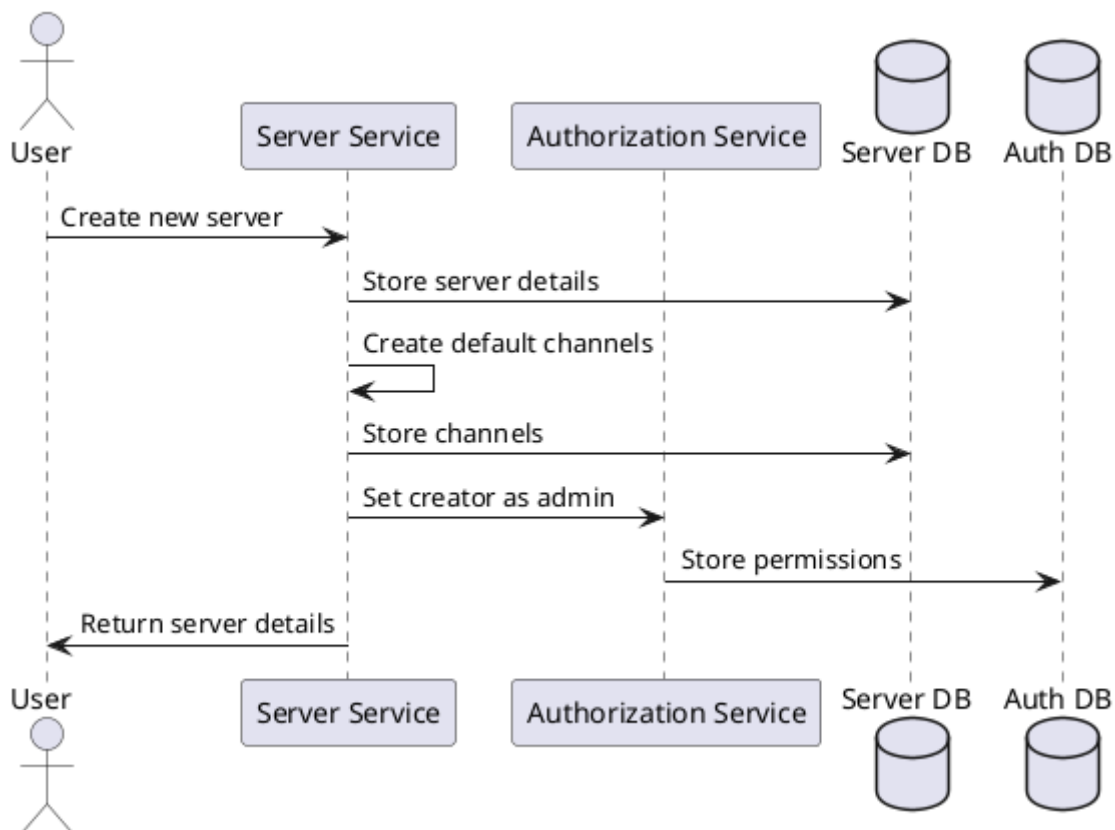
Message Flow

Notification Flow

Network Architecture

This diagram illustrates the network architecture of the Beep platform, showing the security zones and traffic flow.

Authentication Flow

This diagram illustrates the Keycloak authentication flow in the Beep platform.

Keycloak Authentication Flow

User | Frontend Application | Istio Gateway | Keycloak | User Service | User Database | Google Identity Provider
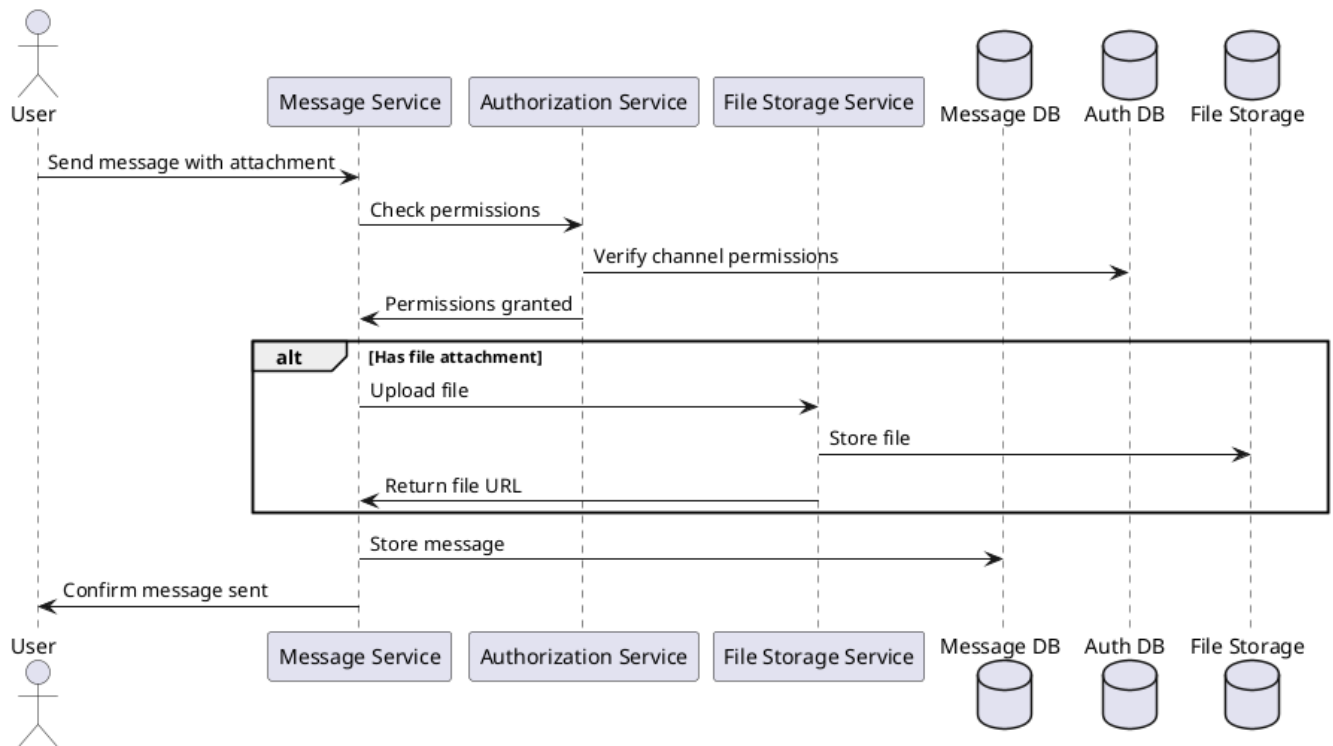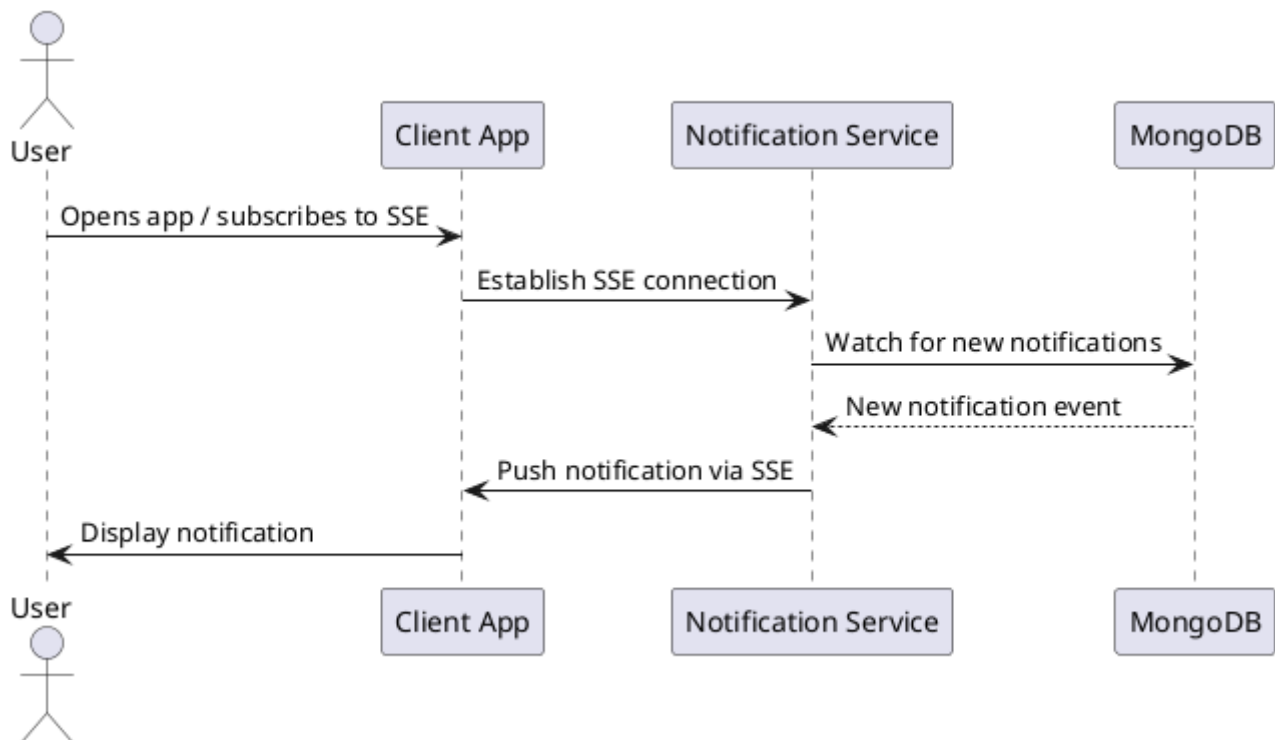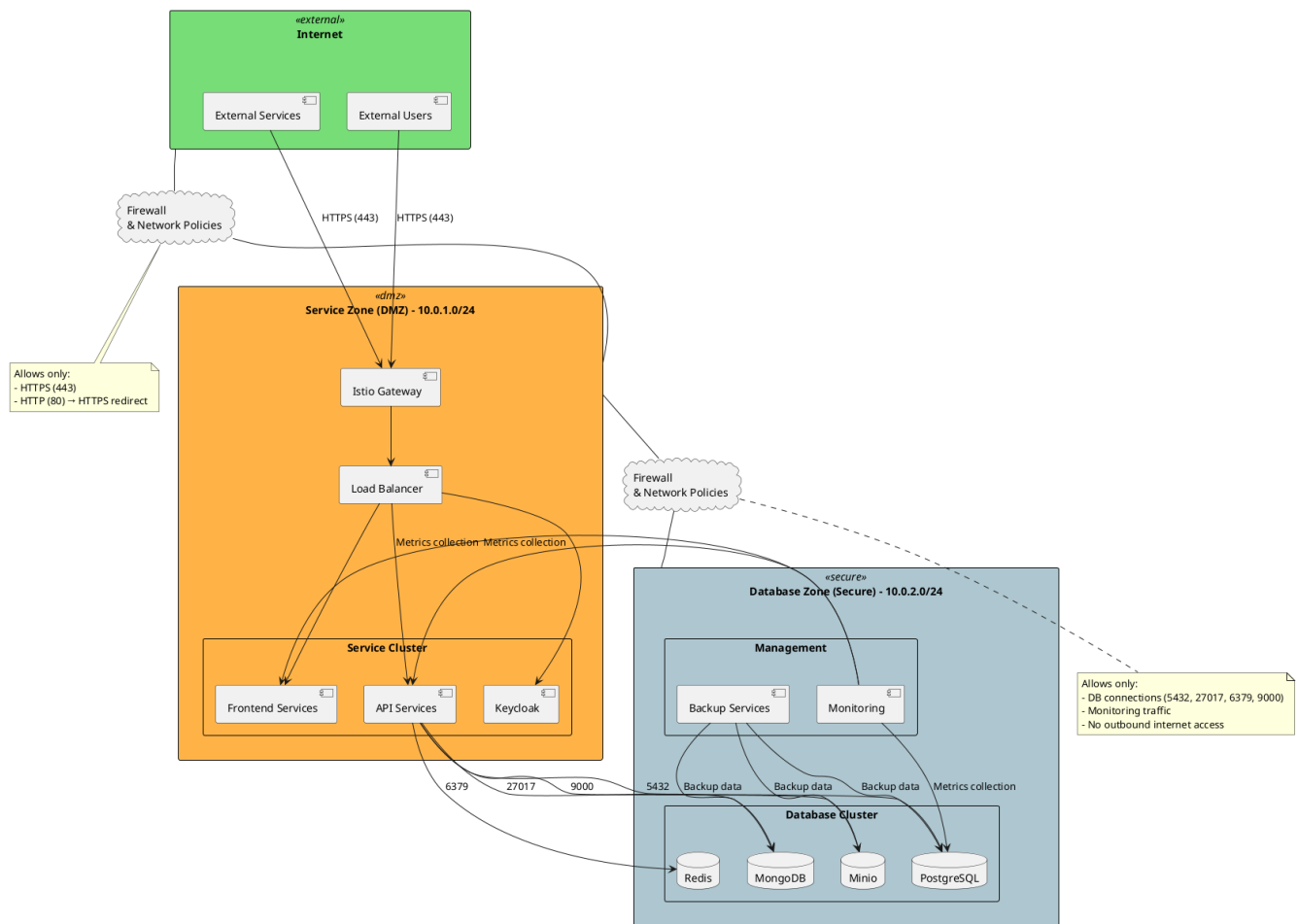
Initial Authentication

- Access protected resource
- Redirect to login
- Login with credentials
- Verify credentials
- Return authorization code
- Authorization code
- Exchange code for tokens
- Access token + Refresh token
- Store tokens in browser

Accessing Protected Resources

- Request protected resource
- Request with access token
- Validate token
- Token validation result

alt [Valid Token]
- Forward request
- Resource data
- Display resource

[Invalid Token]
- 401 Unauthorized
- Request token refresh
- New access token
- Retry with new token

Social Login Flow

- Click "Login with Google"
- Redirect to Keycloak Google login
- Redirect to Google
- Authenticate with Google
- Authentication successful
- Create/update user if needed
- Return authorization code
- Exchange code for tokens
- Access token + Refresh token
- Store tokens in browser

User | Frontend Application | Istio Gateway | Keycloak | User Service | User Database | Google Identity Provider